UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/858,336	05/15/2001	Philip R. Patterson	P0366	1102

23735	7590	07/06/2004

DIGIMARC CORPORATION
19801 SW 72ND AVENUE
SUITE 250
TUALATIN, OR 97062

EXAMINER
WANG, JIN CHENG

ART UNIT	PAPER NUMBER
2672	12

DATE MAILED: 07/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/858,336	PATTERSON ET AL.
	Examiner	Art Unit
	Jin-Cheng Wang	2672

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 March 2004*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9-29* is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a)☐ All　b)☐ Some * c)☐ None of:

　　　　1.☐ Certified copies of the priority documents have been received.

　　　　2.☐ Certified copies of the priority documents have been received in Application No. _____.

　　　　3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
　　　　　　application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
　　Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
　　Paper No(s)/Mail Date _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

U.S. Patent and Trademark Office

PTOL-326 (Rev. 1-04)　　　　　　　　Office Action Summary　　　　　　　　Part of Paper No./Mail Date 12

DETAILED ACTION

Response to Amendment

1.   The amendment filed on 3/26/2004 has been entered. Claims 1-8 have been cancelled.

Claims 9-12, 15-18, 22-23, and 28 have been amended. Claims 9-29 are pending in the

application.

Claim Rejections - 35 USC § 102

2.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed
> in the United States before the invention by the applicant for patent or (2) a patent granted on an application for
> patent by another filed in the United States before the invention by the applicant for patent, except that an
> international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this
> subsection of an application filed in the United States only if the international application designated the United
> States and was published under Article 21(2) of such treaty in the English language.

3.   Claims 9-14 are rejected under 35 U.S.C. 102(e) as being anticipated by Zhao et al. U.S.

Pat. No. 6,141,753 (hereinafter Zhao).

4.   Claim 9:

Zhao teaches a method for managing images, the images including a first image

comprising a first identifier steganographically embedded in the first image in the form of a

digital watermark, said method comprising:

Retrieving the first image from a database (e.g., retrieving the digital representation with

the first fingerprint watermark stored in work storage 105; column 7-8 and 11);

Altering the first image to create a second image (e.g., removing all but the two most recent fingerprint watermarks when it stores the revised digital representation in work storage 105; column 7-8);

Steganographically embedding a second identifier in the second image in the form of a digital watermark (e.g., steganographically embedding the encryption keys including the new and old public watermarks, and/or secret owner identifier watermarks, and/or two symmetrical keys, in the modified digital representation before distribution to a new user; column 5-6; 7-8 and 11);

Associating the second image in the database with the first identifier (e.g., the second image with a new key is stored in the work storage 105 and is associated with the first fingerprint watermark because the second image has the first fingerprint watermark embedded within it; column 7-8).

Claim 10:

The claim 10 encompasses the same scope of invention as that of claim 9 except additional claimed limitation of removing the first identifier from the second image. However, Zhao further discloses the claimed limitation of removing the first identifier from the second image (e.g., Zhao teaches removing all but the two most recent fingerprint watermarks when it stores the revised digital representation in work storage 105; column 7-8).

Claim 11:

The claim 11 encompasses the same scope of invention as that of claim 9 except

additional claimed limitation of altering the first identifier in the second image. However, Zhao

further discloses the claimed limitation of altering the first identifier in the second image (e.g.,

Zhao teaches removing all but the two most recent fingerprint watermarks when it stores the

revised digital representation in work storage 105 and thereby at least one of the two fingerprint

watermarks associated with the second image is altered; column 7-8).

Claim 12:

The claim 12 encompasses the same scope of invention as that of claim 9 except

additional claimed limitation of storing information related to the first image in the database.

However, Zhao further discloses the claimed limitation of storing information related to the first

image in the database (e.g., the copy server maintains a database of transactions, user identifiers,

and keys. The copy server will use the user identifier and a transaction identifier to locate the re-

encryption key that was downloaded to copy client with the digital representation; column 7-8).

Claim 13:

The claim 13 encompasses the same scope of invention as that of claim 12 except

additional claimed limitation of the related information comprising at least one of metadata,

location, date, permission level, security access levels, analyst comments, notes, files, and past

usage information. However, Zhao further discloses the claimed limitation of the related

information comprising at least one of metadata, location, date, permission level, security access

levels, analyst comments, notes, files, and past usage information (such as use limitation or use

information, permission for various uses; column 5-6, 7-8 and 10).

Claim 14:

The claim 14 encompasses the same scope of invention as that of claim 13 except

additional claimed limitation of the database comprising a plurality of databases.

However, Zhao further discloses the claimed limitation of the database comprising a

plurality of databases (the database storing the identifiers and keys and the database storing the

digital representation in the work storage 105; column 7-8).

5.   Claims 15-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Stefik et al.

U.S. Pat. No. 6,233,684 (hereinafter Stefik).

6.   Claim 15:

Stefik teaches a method to monitor images in a system, the system comprising at least a

first user terminal to communicate with a second user terminal and with a database, the images

comprising at least a first image digitally watermarked to include a first identifier, said method

comprising:

Determining a security level (e.g., a security level associated with a usage right in a set of

usage rights for the same digital work) associated with the first image (the first image being the

digital work in an encrypted form; column 9, 12-15);

Comparing the first image security level (set of usage rights associated with the same

digital work wherein the watermark are embedded in the digital work in an encrypted form; the

digital work having different levels of encryption and "scrambling"; column 12-15 and 17) with

a user security level (*e.g., consumer must have an authorizing digital license to access or copy or*

transfer the digital work to avoid unauthorized copying and the consumer possesses a digital

certificate which contains the watermark information; security and watermark capabilities of the

user's terminal are checked; column 12-15 and 17); and

Allowing access (by the consumer or distributor) to the first image (e.g., the digital work)

based on a result of said comparison step (*e.g., by comparing the watermark information in the*

consumer's digital certificate with the watermark information in the digital work identifying the

usage rights, unauthorized usage of the digital work can be prevented and authorized usage is

allowed; the digital work is then decrypted and downloaded into the user's terminal; column 9,

12-15 and 17).

Claim 16:

The claim 16 encompasses the same scope of invention as that of claim 15 except

additional claimed limitation of recording a transmission in the database of the first image from

the first user terminal to the second user terminal.

However, Stefik further discloses the claimed limitation of recording a transmission in

the database of the first image from the first user terminal to the second user terminal (*e.g.,*

column 9, 12-15 wherein the second user terminal is the consumer's terminal or the printer

terminal and the first user terminal is the publisher or distributor's user terminal wherein the

billing records are kept in the Financial Clearinghouse and Credit Servers).

Claim 17:

The claim 17 encompasses the same scope of invention as that of claim 15 except

additional claimed limitation of decoding the digital watermark to determine the first identifier

and interrogating the database with the first identifier to retrieve the security level.

However, Stefik further discloses the claimed limitation of decoding the digital

watermark to determine the first identifier (e.g., watermark embedded into the digital work) and

interrogating the database with the first identifier to retrieve the security level (*e.g., interrogating*

the publisher's or the distributor's repository which encrypts the document using DES or some

other encryption code and the encryption uses a key length that is compatible with requirements

of security and legal constraints; and the distributor repository sends the encrypted document

and the envelope containing the key along to the consumers workstation wherein the embedded

data is extracted from the watermark and decoded. The data extracted is then used to identify

who and where the unauthorized reproduction of the digital work came from. Moreover the

consumer workstation has a program that decrypts the digital page and sends it to the printer

with watermarks; column 9, 12-16).

Claim 18:

The claim 18 encompasses the same scope of invention as that of claim 15 except

additional claimed limitation that the first image's digital watermark includes security level data,

and wherein the determining step comprises the step of decoding the digital watermark to

determine the security level.

However, Stefik further discloses the claimed limitation that the first image's digital

watermark includes security level data (a set of usage rights embedded as watermark in the

digital work, column 9, 12-15), and wherein the determining step comprises the step of decoding

the digital watermark to determine the security level (*e.g., decrypting the digital work by the*

decryption means to determine the security level; interrogating the publisher's or the

distributor's repository which encrypts the document using DES or some other encryption code

and the encryption uses a key length that is compatible with requirements of security and legal

constraints; and the distributor repository sends the encrypted document and the envelope

containing the key along to the consumers workstation wherein the embedded data is extracted

from the watermark and decoded. The data extracted is then used to identify who and where the

unauthorized reproduction of the digital work came from. Moreover the consumer workstation

has a program that decrypts the digital page and sends it to the printer with watermarks; column

9, 12-16).

Claim 19:

The claim 19 encompasses the same scope of invention as that of claim 15 except

additional claimed limitation that the user security level comprises at least one of a security level

for a user and a security level for a user terminal.

However, Stefik further discloses the claimed limitation that the user security level

comprises at least one of a security level for a user and a security level for a user terminal (e.g.,

watermark information in *certificates from the user, the computer itself, and the printer*; column

15).

Claim 20:

The claim 20 encompasses the same scope of invention as that of claim 15 except additional claimed limitation that when the result is a match between the first image security level and the user security level access is allowed.

However, Stefik further discloses the claimed limitation that when the result is a match between the first image security level and the user security level access is allowed (*e.g., by comparing the watermark information in the consumer's digital certificate with the watermark information in the digital work identifying the usage rights, unauthorized usage of the digital work can be prevented and authorized usage is allowed; the digital work is then decrypted and downloaded into the user's terminal; column 9, 12-15 and 17*).

Claim 21:

The claim 21 encompasses the same scope of invention as that of claim 15 except additional claimed limitation that the match indicates that the user security level is equal to or greater than the first image security level.

However, Stefik further discloses the claimed limitation that the match indicates that the user security level is equal to or greater than the first image security level (e.g., it is required that the user or consumer of the digital work needs the identification certificates to access the digital work in the publisher's or distributor's terminal; column 9, 12-15 and 17).

Claim 22:

The claim 22 encompasses the same scope of invention as that of claim 15 except

additional claimed limitation of recording access to the image.

However, Stefik further discloses the claimed limitation of recording access to the image

(e.g., trust box reports billing to a Financial Clearinghouse and Credit Servers which keeps the

billing records; column 9, 12-15).

7.   Claim 23:

Stefik teaches a system comprising:

A first user terminal (e.g., the publisher's terminal);

A second user terminal (e.g., the consumer's terminal along with the trusted printer

having proper security levels and watermark capabilities; column 9, 12-15 and 17);

A database (the repository having a list of digital works), wherein the first user terminal

and the second user terminal are in communication, and the first user terminal and the second

user terminal are each in communication with the database (the repository having a list of digital

works; figures 1 and 5); and

A gatekeeper (e.g., the on-line distributor's terminal and/or the publisher's terminal in

combination with the Credit Server and Billing Clearinghouse; Figures 1 and 5) to regulate the

flow of at least a first image between the first user terminal (the digital work in an encrypted

form at the publisher's terminal) and the second user terminal (the consumer's terminal), wherein

the first image comprises at least a first digital watermark (the encrypted digital work with

watermarks) including a first identifier, said gatekeeper to determine a security level associated

with the first image (by decrypting the digital work), compare the first image security level with

a user security level, and to allow access by the second user terminal to the first image based on a

result of the comparison (*by comparing the watermark information in the consumer's digital*

certificate with the watermark information in the digital work identifying the usage rights,

unauthorized usage of the digital work can be prevented and authorized usage is allowed; the

digital work is then decrypted and downloaded into the user's terminal; column 9, 12-15 and

17).

Claim 24:

The claim 24 encompasses the same scope of invention as that of claim 23 except

additional claimed limitation that the gatekeeper records in the database a transmission of the

first image from the first user terminal to the second user terminal.

However, Stefik further discloses the claimed limitation that the gatekeeper records in the

database a transmission of the first image from the first user terminal to the second user terminal

(e.g., billing records are kept in Financial Clearinghouse and Credit Servers; column 9, 12-15).

Claim 25:

The claim 25 encompasses the same scope of invention as that of claim 23 except

additional claimed limitation that the gatekeeper comprises software to decode the digital

watermark to determine the first identifier, and to interrogate the database with the first identifier

to retrieve the security level.

However, Stefik further discloses the claimed limitation that the gatekeeper comprises

software (the decryption means to decrypt the watermark and/or the extraction means for

extracting the embedded data from the watermark) to decode the digital watermark to determine

the first identifier (column 9, 12-15), and to interrogate the database with the first identifier to

retrieve the security level (*e.g., interrogating the publisher's or the distributor's repository*

which encrypts the document using DES or some other encryption code and the encryption uses

a key length that is compatible with requirements of security and legal constraints; and the

distributor repository sends the encrypted document and the envelope containing the key along

to the consumers workstation wherein the embedded data is extracted from the watermark and

decoded. The data extracted is then used to identify who and where the unauthorized

reproduction of the digital work came from. Moreover the consumer workstation has a program

that decrypts the digital page and sends it to the printer with watermarks; column 9, 12-16).

Claim 26:

The claim 26 encompasses the same scope of invention as that of claim 23 except

additional claimed limitation that the first image digital watermark includes security level data,

and wherein the gatekeeper comprises software code to decode the digital watermark to

determine the security level data.

However, Stefik further discloses the claimed limitation that the first image digital

watermark includes security level data (e.g., different levels of encryption and "scrambling";

column 17), and wherein the gatekeeper comprises software code to decode the digital

watermark to determine the security level data (e.g., the embedded data is extracted from the

watermark and decoded by the means for extraction of the watermark data; Figure 13 and

column 9, 12-15 and 17).

Claim 27:

The claim 27 encompasses the same scope of invention as that of claim 23 except

additional claimed limitation that the user security level comprises at least one of a security level

for a user and a security level for a user terminal.

However, Stefik further discloses the claimed limitation that the user security level

comprises at least one of a security level for a user and a security level for a user terminal (e.g.,

watermark information in *certificates from the user, the computer itself, and the printer*; column

15).

8.   Claim 28:

Stefik teaches a module for use in a network comprising at least a first terminal in

communication with a database, said module to monitor the flow of at least a first image at a first

network location, the first image comprising at least a first digital watermark including a first

identifier, said module comprising:

Means for determining a security level associated with the first image (security levels

associated with the digital work; column 9, 12-15 and 17);

Means for comparing a first image security level with a user security level (*e.g.,*

consumer must have an authorizing digital license to access or copy or transfer the digital work

to avoid unauthorized copying and the consumer possesses a digital certificate which contains

the watermark information; security and watermark capabilities of the user's terminal are

checked; column 12-15 and 17); and

Means for allowing access to the first image based on a result of said comparison step

(*e.g., by comparing the watermark information in the consumer's digital certificate with the*

watermark information in the digital work identifying the usage rights, unauthorized usage of the

digital work can be prevented and authorized usage is allowed; the digital work is then

decrypted and downloaded into the user's terminal; column 9, 12-15 and 17).

Claim 29:

The claim 29 encompasses the same scope of invention as that of claim 28 except

additional claimed limitation of a fragile watermark. However, Stefik further discloses the

claimed limitation of a fragile watermark (e.g., column 1-2, 9, 12-15 and 17).

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Jin-Cheng Wang whose telephone number is (703) 605-1213.

The examiner can normally be reached on 8:00 - 6:30 (Mon-Thu).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Mike Razavi can be reached on (703) 305-4713. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jcw

MICHAEL RAZAVI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600